REMARKS

This communication is a full and timely response to the aforementioned final Office Action dated February 11, 2009 and the Advisory Action dated August 19, 2009. By this communication, claims 1-3, 5, 7-9, 11, 17-20, 22-24, 28, 29, 31 and 32 are amended, and claim 30 is cancelled. Claims 4, 6, 10, 12 and 33 are not amended and remain in the application. Therefore, claims 1-12, 17-20, 22-24 and 28, 29 and 31-33 are pending in the application. Claims 1, 7, 17 and 31 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the foregoing amendments and the following remarks.

I. Rejections Under 35 U.S.C. § 112

A. Claims 31-33 were rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement. This rejection was traversed in the Response to Final Rejection filed on August 3, 2009.

In the Advisory Action, the Office acknowledged the impropriety of this rejection and indicated that the written description rejection of claims 31-33 would be withdrawn.

B. Claim 32 was rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. The Office continues to object to the breadth of claim 32, rather than identify any feature in claim 32 which would be *indefinite* to one skilled in the art. Applicant maintains that the rejection of claim 32 under 35 U.S.C. § 112, second paragraph, is impermissibly based on the Office's objection to the breadth of the claim.

Nevertheless, to render this rejection moot, claim 32 has been amended to recite that "the computing device is a printer," to address the Office's concerns with the breadth of the phrase "functions as a printer." One skilled in the art would understand the unambiguous meaning of the phrase "the computing device is a printer."

II. Rejections Under 35 U.S.C. § 103

Claims 1, 4, 5, 7, 10, 12, 17, 20, 22-24 and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters (U.S. Patent Application Publication No. 2004/0088548, hereinafter "Smetters") in view of Benussi et al. (U.S. Patent Application Publication No. 2001/0044898, hereinafter "Benussi").

The Office continues to allege that Smetters discloses something which it does not, by selectively cobbling together bits and pieces of the disclosure of Smetters and disregarding any portion which refutes the Office's mischaracterization of the *actual* disclosure of Smetters. In view of the Office's interpretation that the examination requirement to consider a reference as a whole (see MPEP 2141.03.VI) can be disregarded, independent claims 1, 7, 17 and 31 have each been amended to recite additional distinguishing features over the applied references.

An exemplary embodiment of the present invention provides a communication system in which an image processing apparatus 100 and a client 200 communicate with each other through a network 300 (see Figure 1).

As shown in Figure 2, for example, the image processing apparatus 100 includes a first storage device 118, is configured to create a root certificate 126. The root certificate 126 includes a public key paired with a private key and is signed with the private key. Accordingly, the image processing apparatus 100 comprises a root certificate creator which creates the root certificate 126, which includes a public key paired with a private key, and which is signed with the private key.

The image processing apparatus 100 also includes a second certificate creator 124 which creates a second certificate 128. The second certificate creator 124 creates the second certificate 128 when a connection for communication with the image processing apparatus 100 is requested by the client 200. The second certificate 128 designates the root certificate 126 as a certificate authority at a higher level and is signed with the private key used to sign the root certificate 126. The image processing apparatus 100 comprises a communication device 106 which transmits the second certificate 128 created by the certificate creator 124 to the client 200 (see Figure 2).

With reference to Figure 3, for example, the client 200 includes a storage device 214 which has stored therein, before the connection for communication is

requested to the image processing apparatus 100, the root certificate 222 (126) created by the root certificate creator 126 of the image processing apparatus 100. The client 200 also comprises a verifier which verifies the signature of the second certificate 128 received from the image processing apparatus 100 with the root certificate 222 (126) already stored in the storage device 214.

Accordingly, the disclosed embodiment provides that the root certificate 222 (126) created by the root certificate creator of the image processing apparatus 100 is also stored in the second storage device 214 of the client 200 before the client 200 requests a connection for communication to the image processing apparatus 100. Therefore, the root certificate 222 (126) is stored in the client 200 prior to initiation of communication between the image processing apparatus 100 and the client 200. Furthermore, the disclosed embodiment provides that the image processing apparatus 100 creates the second certificate 128, which designates the root certificate 222 (126) as a certificate authority at a higher level and which is signed with the private key used to sign the root certificate 222 (126), when the client 200 requests the image processing apparatus 100 for a connection for communication therebetween (see, for example, paragraph [0028] on pages 11 and 12 of the specification). Accordingly, the disclosed embodiment provides that the root certificate 222 (126) created by the image processing apparatus 100 is installed in the client 200 prior to an initiation of communication between the client 200 and image processing apparatus 100, and then, after the client 200 requests a connection for communication to the image processing apparatus 100, the image processing apparatus 100 creates and sends the second certificate 128 to the client 200.

The above-described exemplary embodiment provides an advantageous aspect of enabling the image processing apparatus 100 and the client 200 to securely communicate with each other through the network 300, without requiring either the image processing apparatus 100 or the client 200 to purchase an electronic certificate from an authority outside the network, such as a certificate authority (CA). This is achieved because the root certificate 126 created by the image processing apparatus 100 is also stored in the second storage device 214 of the client 200, prior to an initiation of communication between the image processing

apparatus 100 and the client 200. After the client 200 requests a connection for communication to the image processing apparatus 100 and receives the second certificate 128 from the image processing apparatus 100, the verifier of the client 200 can then verify the signature of the received second certificate 128 with the root certificate 222 (126) that is already stored in the storage device 214 of the client 200. Consequently, the client 200 does not require a certificate issued by a third-party CA or a CA outside the network to verify the second certificate 128 received from the image processing apparatus 100.

(1) Independent Claims 1, 7, 17 and 31

Independent claims 1, 7, 17 and 31 each recite various features of the above-described exemplary embodiment.

Claim 1 recites a communication system in which an image processing apparatus and a client communicate data with each other through a network. Claim 1 recites that the image processing apparatus comprises a root certificate creator which creates a root certificate including a public key paired with a private key and signed with the private key. In addition, claim 1 recites that the device comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate. Claim 1 also recites that the client comprises a storage device which has stored therein, before the connection for communication is requested to the image processing apparatus, the root certificate created by the root certificate creator of the image processing apparatus.

Claim 7 recites a communication method for a communication system in which an image processing apparatus and a client communicate data with each other through a network, wherein the image processing apparatus creates a root certificate including a public key paired with a private key and being signed with the private key. The method of claim 7 also comprises the client installing the root certificate which is created by the image processing apparatus, prior to the client requesting a connection for communication to the image processing apparatus. In addition, the method of claim 7 includes the device creating, when a connection for

communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being singed with the private key used to sign the root certificate when data is sent to the client.

Claim 17 recites an image processing apparatus to be used in a communication system in which the image processing apparatus and a client communicate with each other through a network, the image processing apparatus sends information to the client, and the client uses the information to communicate with the image processing apparatus . The image processing apparatus of claim 17 comprises a root certificate creator which creates a root certificate including a pair of a public key and a private key and being signed with the private key. In addition, the image processing apparatus of claim 17 comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to the sign the root certificate. The image processing apparatus of claim 17 also comprises an interface which sends the root certificate to the client before the connection for communication is requested, and sends, after the root certificate created by the root certificate creator is installed in the client, the second certificate for verification of the information sent from the image processing apparatus.

Claim 31 recites a computer-readable recording medium having a computer program recorded thereon that causes a computing device to perform operations of storing a pair of a public key and a private key, creating a root certificate signed with the private key, and sending information and the root certificate created by the computing device and including the public key to the client, before a request for communication is requested by the client. In addition, claim 31 recites that the computer program causes the computing device to perform an operation of creating, when the connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate.

Accordingly, independent claims 1, 7, 17 and 31 each recite that the image processing apparatus (computing device) (1) creates a root certificate that is stored and/or installed in the client before a request for communication is requested by the

client, and (2) creates a second certificate, which designates the root certificate as a certificate authority at a higher level, when a connection for communication is requested by the client.

Applicant respectfully submits that the applied references do not disclose or suggest the above-described features (1) and (2) of independent claims 1, 7, 17 and 31 for at least the following reasons.

Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) then "generates a root certificate 30 for the new space 20, and digitally signs the [root] certificate 30" (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4) (emphasis added).

Smetters discloses that the first device 12(1) then generates a second certificate 40 to be transmitted to a second device 12(2). The first device 12(1) generates the second certificate using either (i) a public key sent from the second device 12(2) to the first device 12(1), or (ii) a public key generated by the first device 12(1) (see paragraph [0034], and step 550 in Figure 6).

Smetters discloses that the first device 12(1) then sends both the root certificate 30 and the second certificate 40 to the second device 12(2). In particular, the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device at the same time after the second certificate 40 is created. The second device 12(2) then stores the received root certificate 30 and second certificate 40 in a memory thereof (see paragraph [0035] and step 600 in Figure 2).

Accordingly, as acknowledged by the Office, Smetters does not disclose or suggest that the second certificate 40 created by the first device 12(1) is stored or installed in the second device 12(2) before the second device 12(2) requests communication to the first device 12(1).

In an attempt to arrive at this feature, the Office applied Benussi. However, Benussi also does not disclose or suggest feature (1) of claims 1, 7, 17 and 31.

On the contrary, Benussi discloses that "the public key of the Root CA is pre-installed in each CB [connectivity box] as the 'Certificate for Root CA' of [pre-installed] parameters 190" (see paragraph [0214], lines 53-55) (emphasis added). Benussi discloses that the Root CA is the "root certificate authority" (see paragraph [0214], lines 26-27).

Accordingly, Benussi discloses that the public key of the Root CA, not the Root CA, is preinstalled in the CB. Furthermore, Benussi discloses that the CB receives the public key of the Root CA from the CSS (communication service system). However, the CSS does not create the Root CA.

Consequently, Benussi does not disclose or suggest that the CB has stored or installed therein a Root CA which is created by the CSS, before a connection for communication is requested to the CSS by the CB.

Accordingly, Benussi does not cure the deficiencies of Smetters for failing to disclose or suggest that (1) the image processing apparatus (computing device) (1) creates a root certificate that is stored and/or installed in the client before a request for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

In addition, Smetters and Benussi do not disclose or suggest that (2) the image processing apparatus (computing device) creates a second certificate which designates the root certificate created by the image processing apparatus (computing device) as a certificate authority at a higher level. The Office alleged that Smetters discloses this feature. This assertion is not supportable.

As discussed above, Smetters discloses that the first device 12(1) generates the second certificate using either (i) a public key sent from the second device 12(2) to the first device 12(1), or (ii) a public key generated by the first device 12(1). Further, the first device 12(1) includes in the second certificate 40 information identifying the location of the shared space 20, which resources in the shared space 20 the second device 12(2) is permitted to access, and whether the second device 12(2) can invite other devices and grant access to the shared space 20 (see paragraph [0034], and step 550 in Figure 6). At no point does Smetters disclose or suggest that the second certificate 40 designates the root certificate 30 as a certificate authority at a higher level.

Furthermore, Benussi discloses that the root CA is possessed by the CSS, which is a server. A server is distinct from an image processing apparatus. Benussi also discloses that a new user purchases a CB (see paragraph [0203]), which has pre-installed therein the public key of the root CA. The CSS does not create the root CA.

Therefore, neither Smetters nor Benussi disclose or suggest that (2) the image processing apparatus (computing device) creates a second certificate which designates the root certificate created by the image processing apparatus (computing device) as a certificate authority at a higher level, as recited in claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 7, 17 and 31 are patentable over Smetters and Benussi, since Smetters and Benussi, either individually or in combination, fail to disclose or suggest features (1) and (2) of claims 1, 7, 17 and 31.

(2) Dependent Claims

Dependent claims 4, 5, 10, 12, 20, 22-24, 28-30, 32 and 33 recite further distinguishing features over Smetters and Benussi.

For example, claim 10 recites that, in the method of claim 7, when the client installs the root certificate, the installation is performed after the root certificate is confirmed by a user. In an attempt to arrive at the features of claim 10, the Office referred to paragraph [0031] of Smetters, which discloses that the operator of the second device 12(2) decides whether to respond to the invitation from the first device 12(1) to gain access to the shared space 20. This does not amount to the features recited in claim 10, because Smetters does not disclose, suggest or contemplate that the operator of the second device 12(2) confirms the root certificate 30 prior to its installation. On the contrary, paragraph [0031] of Smetters merely discloses that the operator 12(2) decides whether he or she wants to gain access to the shared space 20, in response to the invitation message transmitted from the first device 12(1).

Claim 20 recites that the root certificate is stored in the storage device of the client prior to the transmission of the second certificate from the communication device of the image processing apparatus. Claim 23 recites that, in the method of

claim 7, the device sends the second certificate to the client after the root certificate is installed in the client.

As discussed above, a major emphasis of Smetters is for the first device 12(1) to send both the root certificate 30 and the second certificate 40 to the second device 12(2) at the same time. Accordingly, Smetters discloses an opposite technique to the features of claims 20 and 23.

In an attempt to cure the deficiencies of Smetters, the Office has improperly changed a principle of operation of Smetters by applying Benussi. The improper combination of Smetters and Benussi is contrary to well-settled provisions of changing the principle of operation of a reference (see, e.g., *In re Ratti*, 123 USPQ 349 (CCPA 1959); MPEP 2143.01.VI). Therefore, Applicant respectfully submits that the combination of Smetters and Benussi to arrive at the features of claims 20 and 23 is not supportable.

Claim 22 recites that the verifier of the client is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in the second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from the image processing apparatus, and comparing the first and second hash values to determine if they are equal to each other.

The Office asserted that the features recited in claim 22 are disclosed in paragraphs [0041] and [0042] of Smetters. This assertion is not supportable. Paragraphs [0041] and [0042] of Smetters do not disclose or suggest the calculation of the first and second hash values and the subsequent comparison of the first and second hash values, as recited in claim 22. Paragraphs [0041] and [0042] do not disclose or suggest the generation of hash values from either the root certificate 30 or the second certificate 40.

Claims 28 and 29 recite that the client stores the public key of the installed root certificate, prior to the client requesting the connection for communication to the image processing apparatus, and that the client verifies the signature of the second certificate received from the image processing apparatus by decrypting the second certificate with the public key of the root certificate stored in the client.

Smetters and Benussi do not disclose or suggest the features of claims 28 and 29. In particular, as discussed above, Smetters discloses that the second device 12(1) decrypts the second certificate 40 by using the private key that is either sent from the first device 12(1) (when the first device 12(1) generates a new key pair for the second certificate 40) or is already installed in the second device 12(2) (when the second device 12(2) transmits the public key for creation of the second certificate 40). Accordingly, Smetters does not disclose or suggest that the second device 12(2) verifies the signature of the second certificate 40 by decrypting the second certificate 40 with the public key of the root certificate 30.

Furthermore, Benussi does not disclose or suggest any second certificate corresponding to the claimed invention. Therefore, Applicant respectfully submits that claims 28 and 29 recite further distinguishing features over the applied references.

For at least the foregoing reasons, Applicant respectfully submits that Smetters and Benussi, either individually or in combination, do not disclose or suggest the features of dependent claims 10, 20, 22, 23, 28 and 29, in addition to failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, in addition to the patentability of claims 1, 7, 17 and 31 demonstrated above, Applicant respectfully submits that claims 10, 20, 22, 23, 28 and 29 recite further distinguishing features over Smetters and Benussi.

B. Claims 28, 29 and 31 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Smetters in view of Benussi and further in view of Schneier's Applied Cryptography, 2nd Edition (hereinafter "Schneier").

As demonstrated above, neither Smetters nor Benussi disclose or suggest that an the image processing apparatus (computing device) (1) creates a root certificate that is stored and/or installed in the client before a request for communication is requested by the client, and (2) creates a second certificate, which designates the root certificate as a certificate authority at a higher level, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Similarly, Schneier also fails to disclose or suggest these features of claims 1, 7, 17 and 31. Therefore, Schneier cannot cure the deficiencies of Smetters and Benussi. Consequently, no obvious combination of Smetters, Benussi and Schneier would arrive at the subject matter of claims 1, 7, 17 and 31, since Smetters, Benussi and Schneier, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, Applicants respectfully submit that claims 1, 7, 17 and 31 are patentable over Smetters, Benussi and Schneier.

C. Dependent claims 2, 3, 6, 8, 9, 11, 18, 19, 26, 27, 32 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benussi and further in view of one or more of Schneier, Frailong et al. (U.S. Patent No. 6,012,100, hereinafter "Frailong'), Debry (U.S. Patent No. 6,918,042, hereinafter "Debry"), Slick (U.S. Patent Application Publication No. 2004/0109568, hereinafter "Slick"), and Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel").

As demonstrated above, Smetters and Benussi each do not disclose or suggest that the image processing apparatus (computing device) (1) creates a root certificate that is stored and/or installed in the client before a request for communication is requested by the client, and (2) creates a second certificate, which designates the root certificate as a certificate authority at a higher level, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Similarly, Schneier, Frailong, Debry, Slick and Vogel also each fail to disclose or suggest these features of claims 1, 7, 17 and 31. Therefore, Schneier, Frailong, Debry, Slick and Vogel cannot cure the deficiencies of Smetters and Benussi for failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31, since the applied references, either individually or in combination, do not disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, no obvious combination of Smetters, Benussi, Schneier, Frailong, Debry, Slick and Vogel would arrive at the subject matter of the claimed invention, since the applied references, either individually or in combination, fail to disclose or suggest all the recited features of at least claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 7, 17 and 31, as well as claims 2-6, 8-12, 18-20, 22-24, 28, 29, 32 and 33 which depend therefrom, are patentable over the applied references.

The foregoing explanation of the patentability of independent claims 1, 7, 17 and 31 is sufficiently clear such that it is believed to be unnecessary to separately demonstrate the patentability of the dependent claims not specifically addressed above at this time. However, Applicant reserves the right to do should it become appropriate.

III. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this Amendment, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: October 9, 2009

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839